LISTING OF THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (currently amended) An authentication system to verify a password, the system being arranged for coupling to a host for communication therewith, and comprising:

a first storage unit to store an authentication sequence;

a read-only memory unit to store an authentication algorithm;

a microcontroller coupled to said first storage unit, said read-only memory unit, and a web server, wherein said microcontroller is to receive said password and execute said authentication algorithm and wherein said authentication algorithm is to verify said password with said authentication sequence; and

a second storage unit coupled to said microcontroller to store data from said web server and wherein access to said second storage unit is permitted by said microcontroller only if said password has been verified,

wherein the system is arranged to receive data from the web server, via the host, in encrypted form and to decrypt that data before use thereof in the host.

2. (currently amended) The authentication system as recited in claim 1, ~~further comprising a host coupled between said authentication system and said web server,~~ wherein [[said]] the password is received by said microcontroller from said host.

3. (original) The authentication system as recited in claim 2, wherein said read-only memory unit further comprises a shutdown algorithm to shut down said host and said authentication system after a number of incorrect passwords is received by said microcontroller.

4. (original) The authentication system as recited in claim 2, wherein said password is received by said host from said web server.

5. (original) The authentication system as recited in claim 2, wherein said authentication algorithm is hard coded on one of a group consisting of a firmware and a hardware in said microcontroller.

6. (original) The authentication system as recited in claim 5, wherein said second storage unit is a removable storage device.

7. (original) The authentication system as recited in claim 6, wherein said second storage unit uses flash memory.

8. (original) The authentication system as recited in claim 2, wherein said microcontroller and said read-only memory unit are implemented on a single semiconductor chip.

9. (original) The authentication system as recited in claim 8, wherein said first storage unit and said read-only memory unit are incorporated into said microcontroller.

10. (original) The authentication system as recited in claim 1, further comprising an encoder coupled between said microcontroller and said second storage unit, wherein said encoder is to encrypt data that is to be written onto said second storage unit.

11. (original) The authentication system as recited in claim 10, further comprising a decoder coupled between said microcontroller and said second storage unit, wherein said decoder is to decrypt data that is to be read from said second storage unit.

12. (original) The authentication system as recited in claim 11, wherein data stored in said second storage unit is hash-coded.

13. (original) The authentication system as recited in claim 12, wherein said authentication sequence is encrypted.

14. (original) The authentication system as recited in claim 12, wherein said authentication sequence is hash-coded.

15. (original) The authentication system as recited in claim 1, wherein said first storage unit is located within said read-only memory unit and wherein said authentication sequence is hard coded into said first storage unit.

16. (original) The authentication system as recited in claim 15, wherein said second storage area further comprises a public storage area and a private storage area.

17. (original) The authentication system as recited in claim 16, wherein said first storage unit is located within said private storage area of said second storage area.

18. (currently amended) A method for authenticating a password, comprising:

coupling an authentication system to a host for communication therewith;

the system receiving said password;

the system receiving data from a web server, via the host, in encrypted form, wherein said data is stored in a storage unit of the system;

the system providing an authentication sequence;

the system executing an authentication algorithm to verify said password with said authentication sequence, wherein said authentication algorithm is stored on a read-only memory unit of the system; [[and]]

the system permitting access to said data on said storage unit only if said password is verified; and

the system decrypting the data before use in the host.

19. (original) The method for authenticating a password as recited in claim 18, wherein said password is received from said web server.

20. (original) The method for authenticating a password as recited in claim 19, wherein said password is entered by a user.

Claims 21-22 (canceled).